

Title: Pre-Computation and Dual-Pass Modular Arithmetic Operation
Approach to Implement Encryption Protocols Efficiently in Electronic
Integrated Circuits
Inventor(s): Mihailo M. Stojancic, et al.
Serial No.: 09/955,902
Docket No. 50325-0550

1 / 28

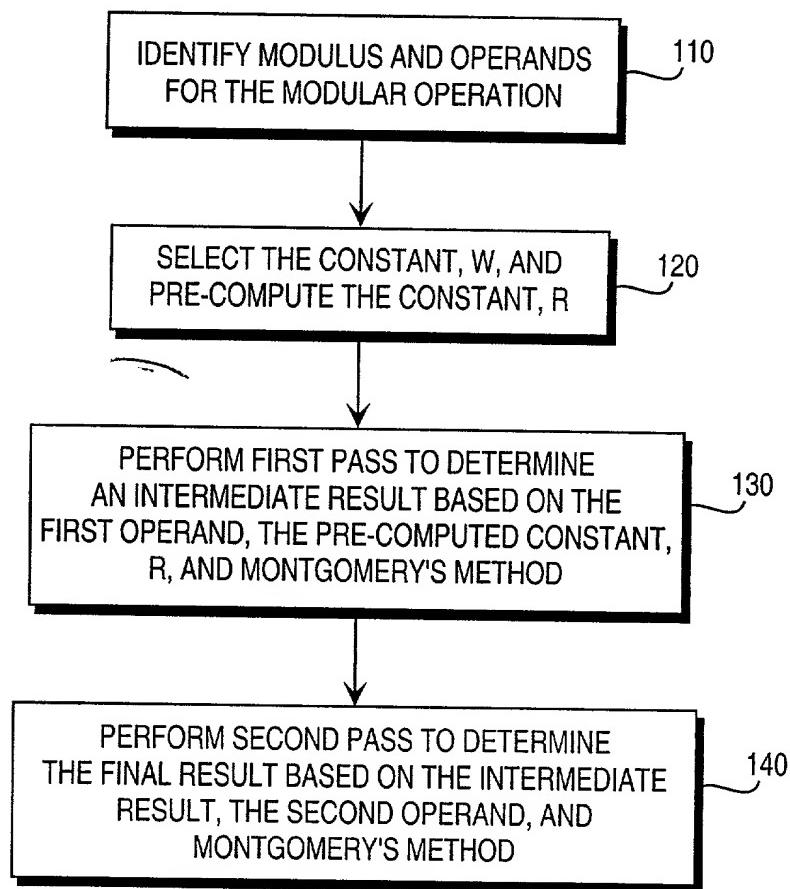


FIG. 1

2 / 28

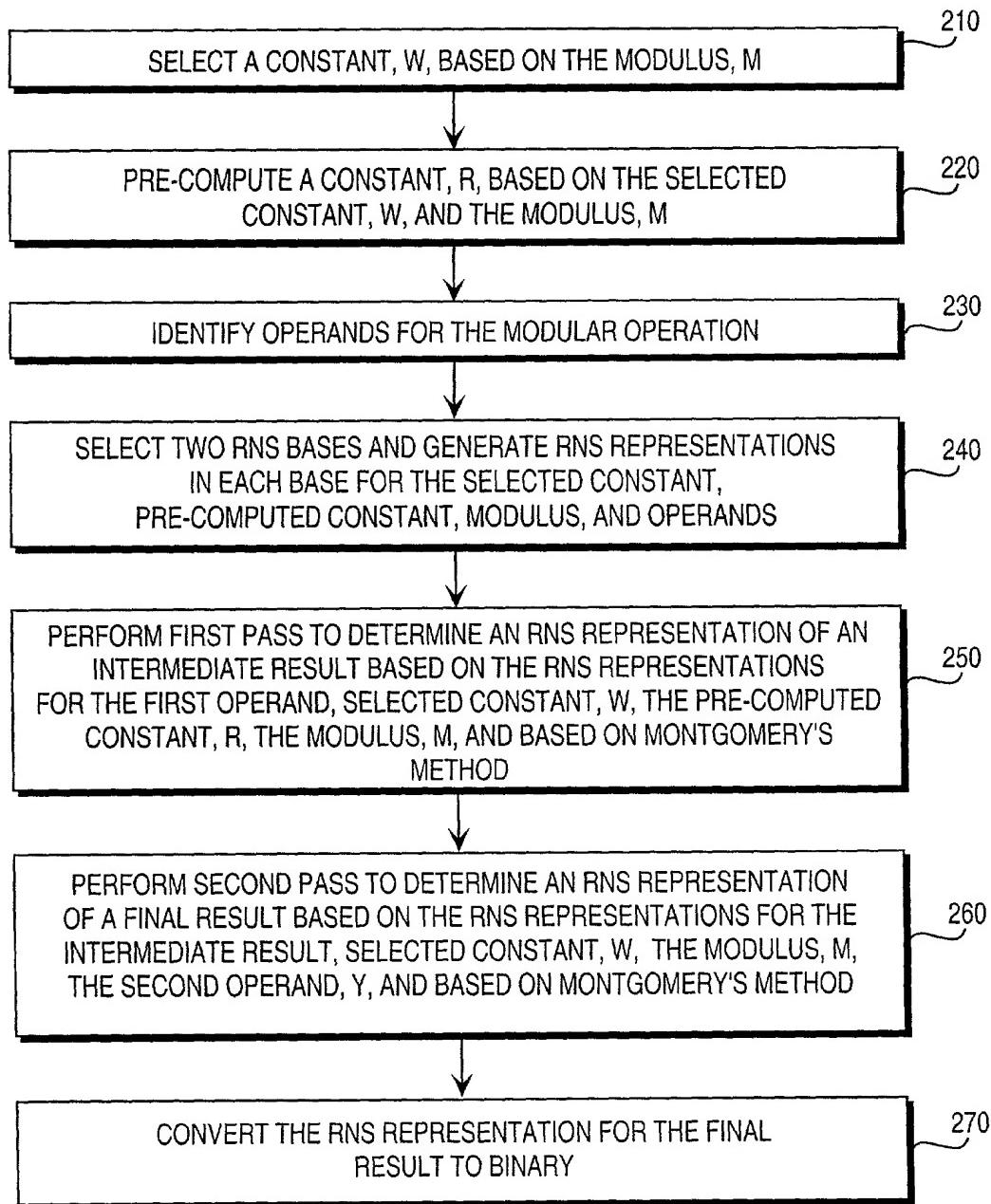


FIG. 2

Title: Pre-Computation and Dual-Pass Modular Arithmetic Operation Approach to Implement Encryption Protocols Efficiently in Electronic Integrated Circuits
Inventor(s): Mihailo M. Stojancic, et al.
Serial No.: 09/955,902
Docket No. 50325-0550

3 / 28

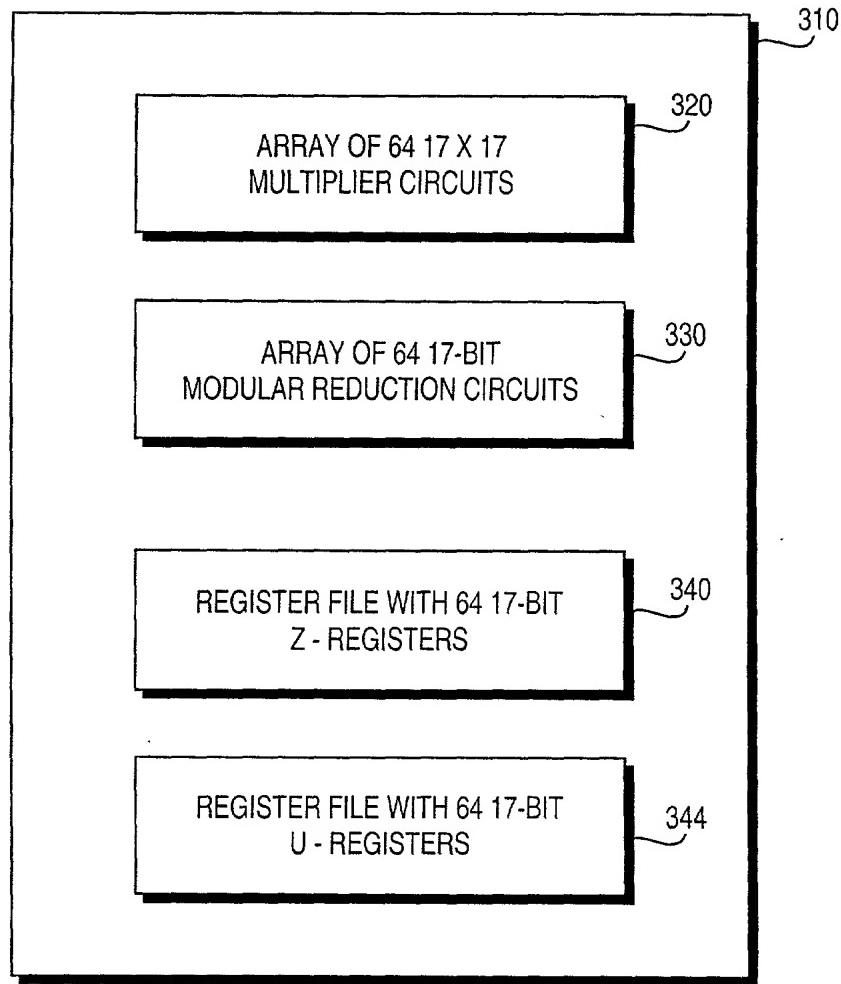


FIG. 3A

Title: Pre-Computation and Dual-Pass Modular Arithmetic Operation Approach to Implement Encryption Protocols Efficiently in Electronic Integrated Circuits
Inventor(s): Mihailo M. Stojancic, et al.
Serial No.: 09/955,902
Docket No. 50325-0550

4 / 28

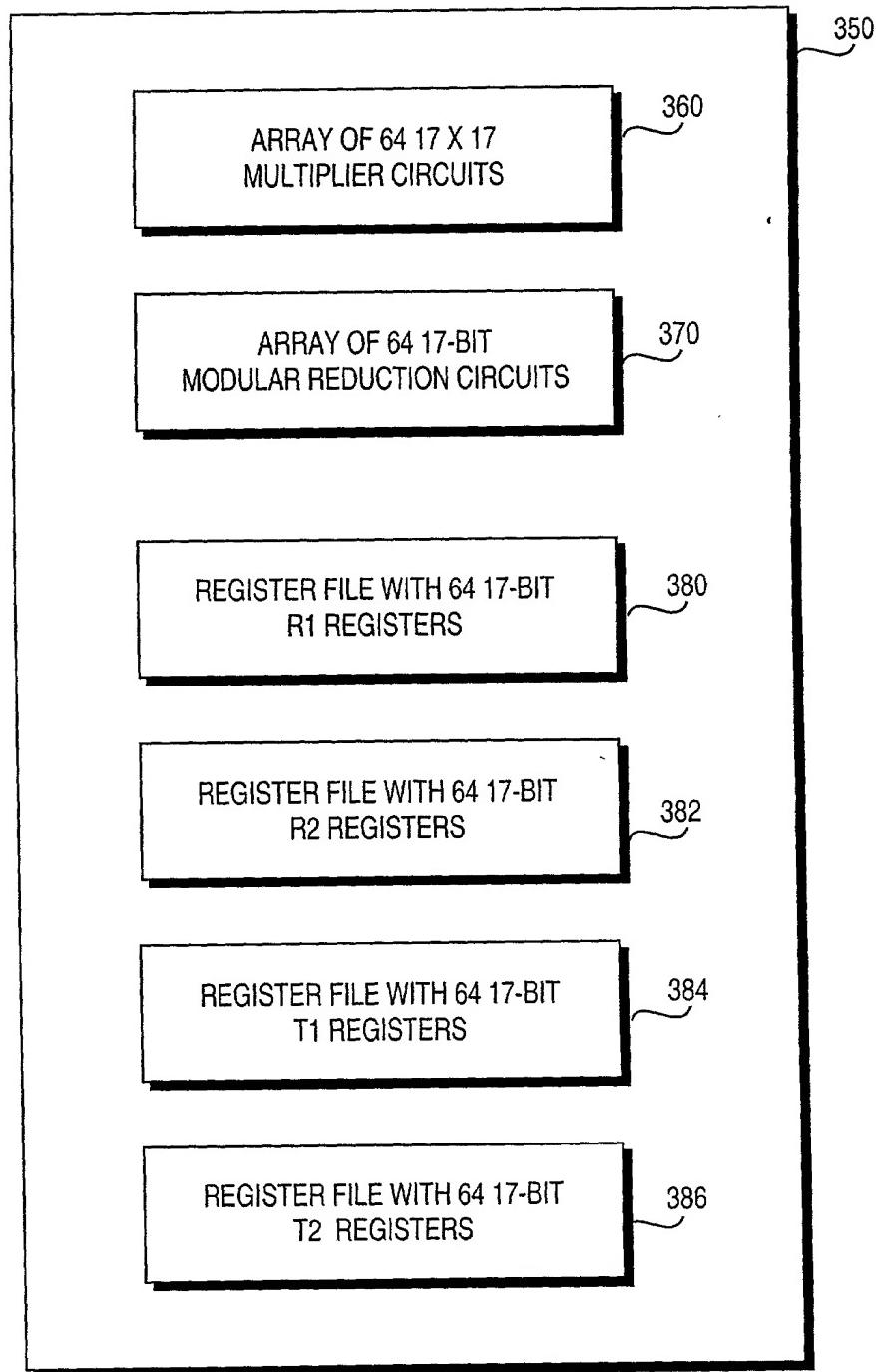


FIG. 3B

5 / 28

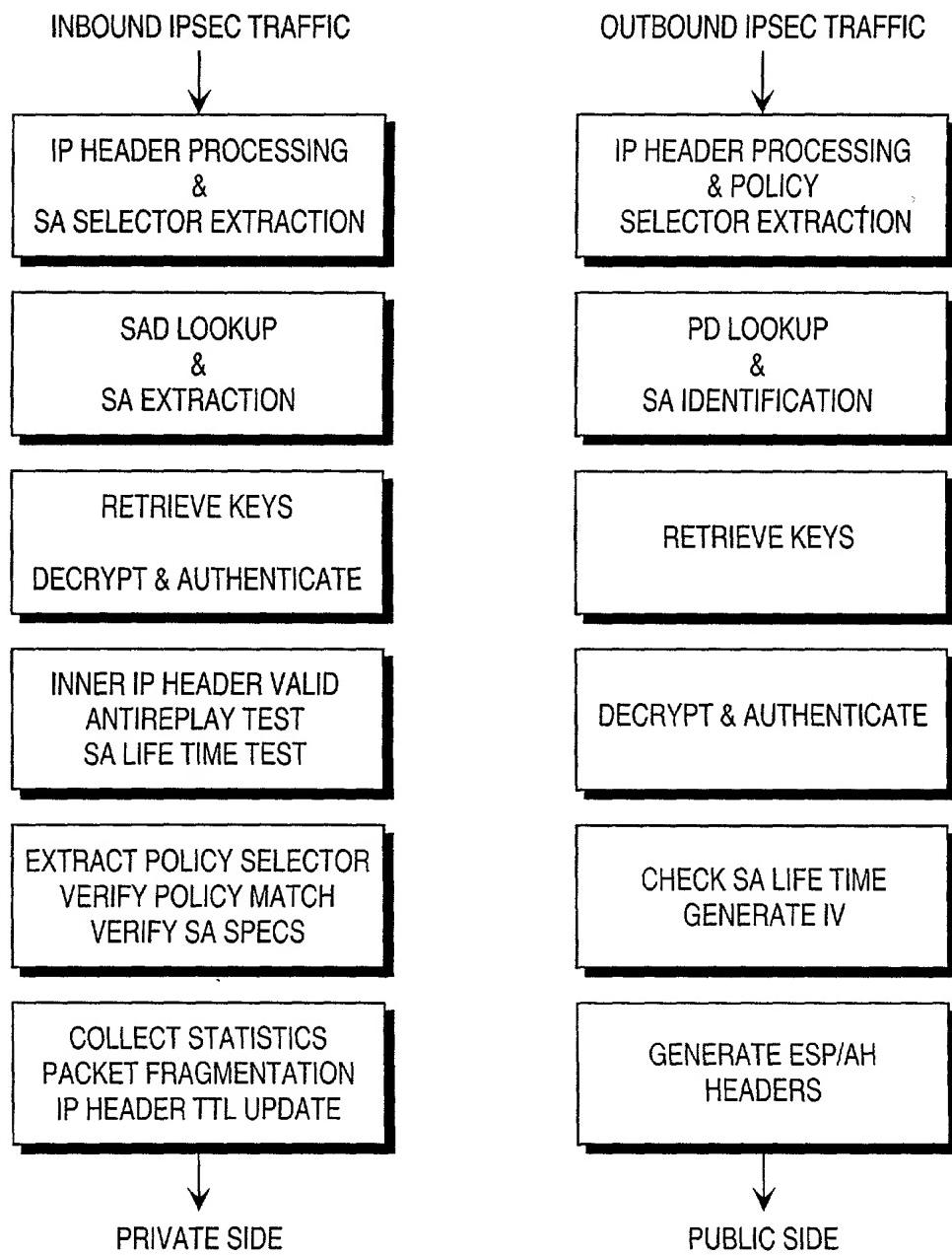
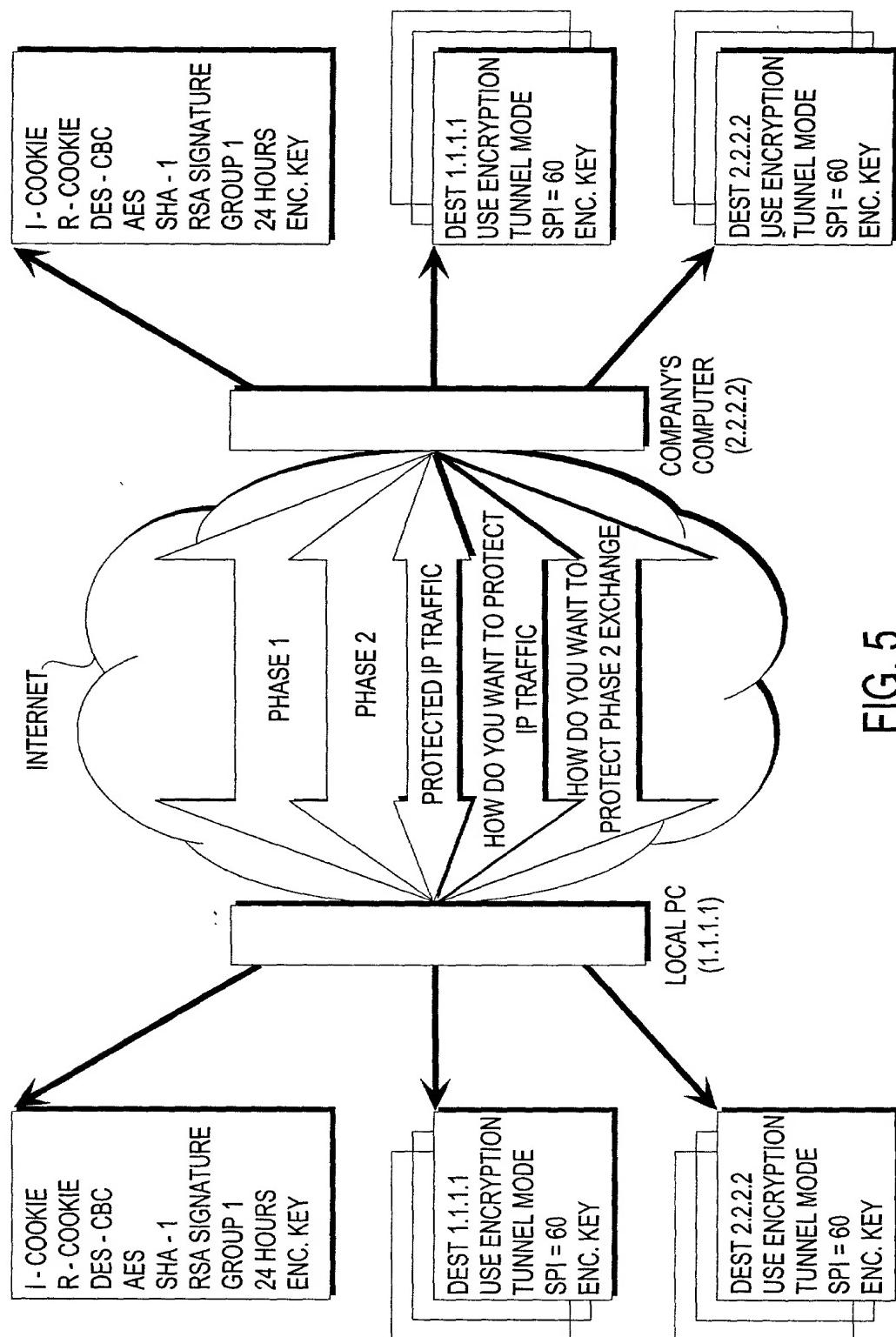


FIG. 4

6 / 28



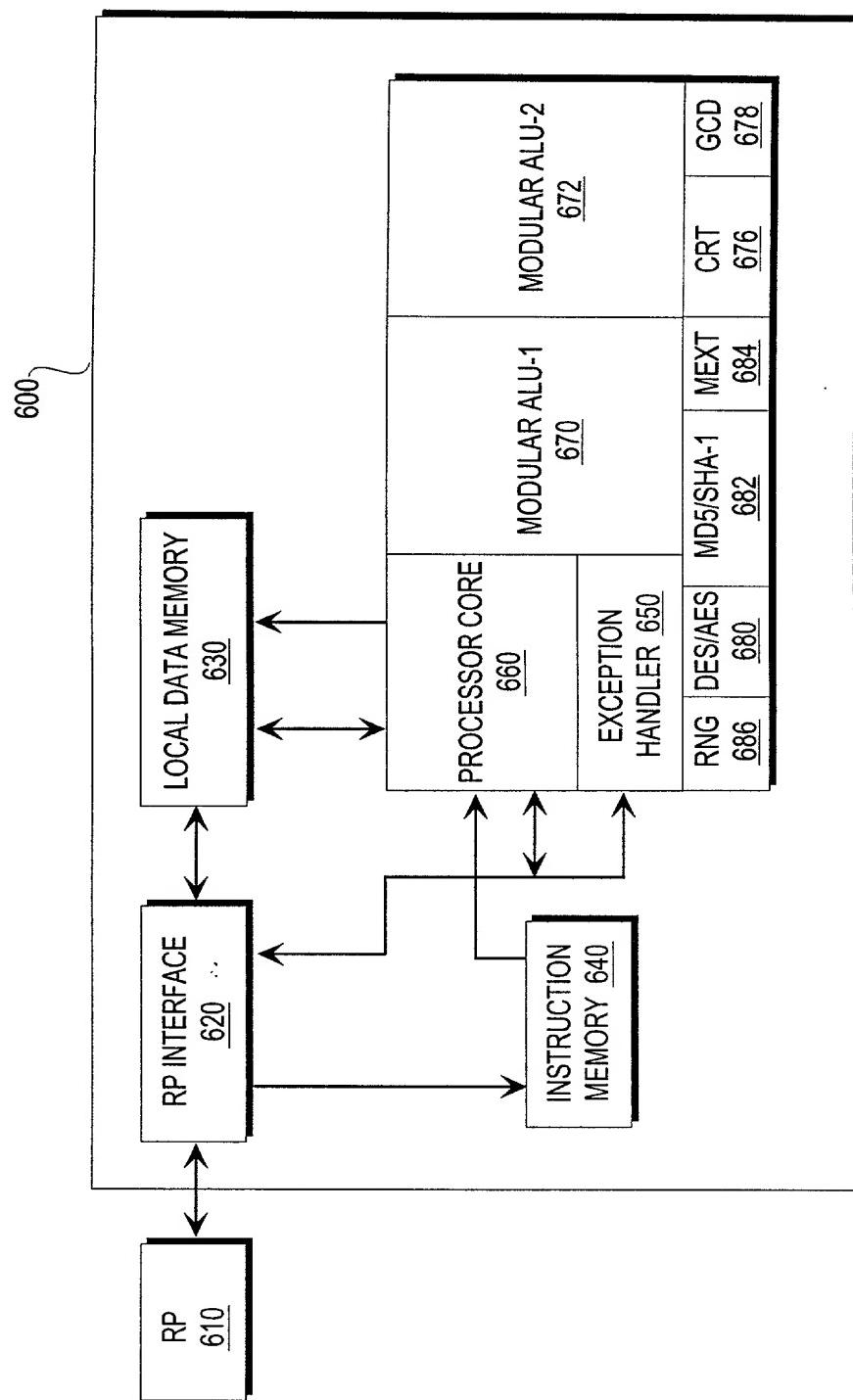


FIG. 6

8 / 28

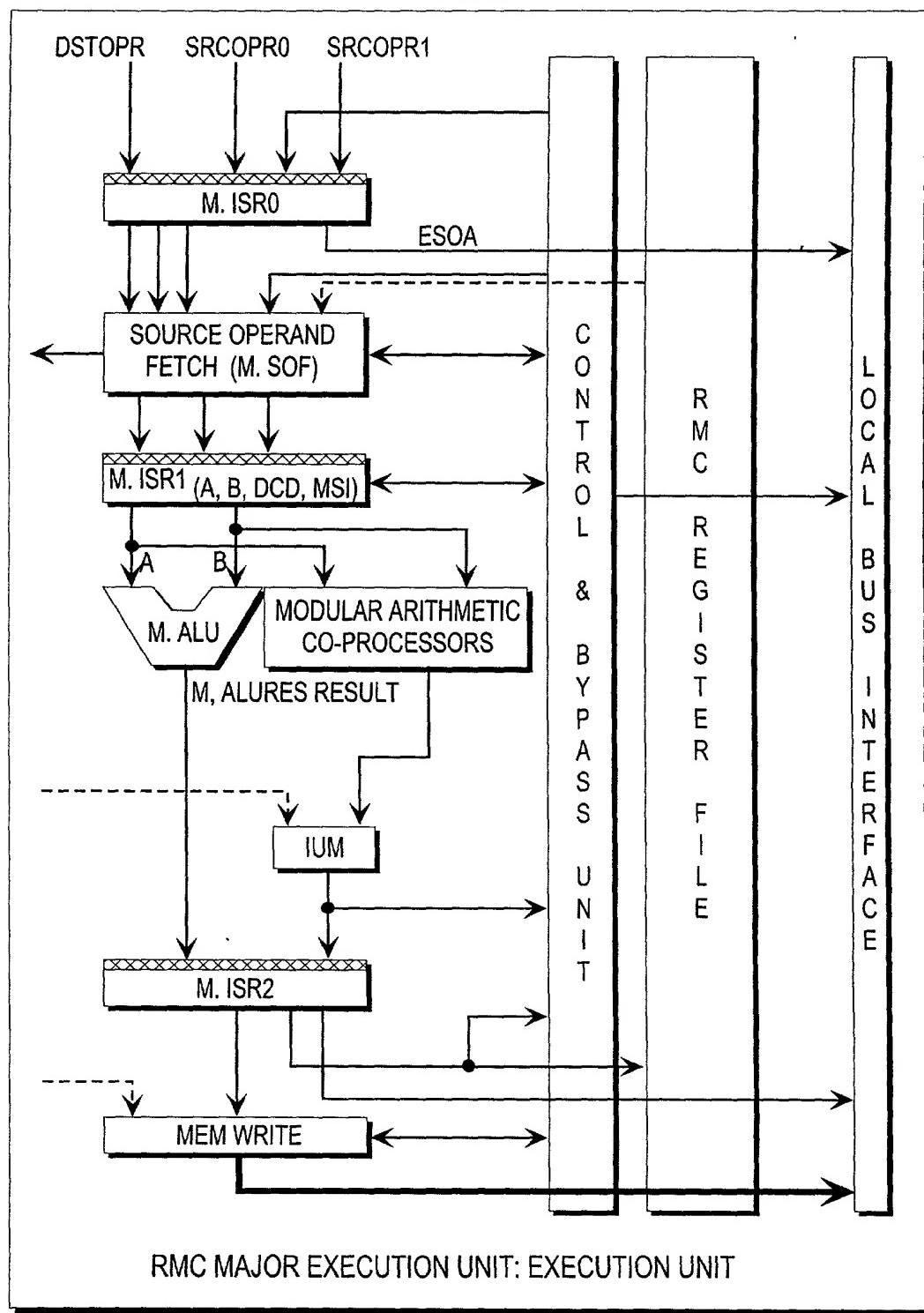


FIG. 7

9 / 28

NOTE: RECTANGULAR BLOCKS ON THE SAME HORIZONTAL LEVEL
 OVERLAP EXECUTION TIMES.

- \leftarrow - SOURCE OVERWRITES DESTINATION REGISTER
- \circledast - MODULAR MULTIPLICATION WITH RESPECT TO W.
- \odot - MODULAR MULTIPLICATION WITH RESPECT TO V.
- \angle - RNS CONVERSION

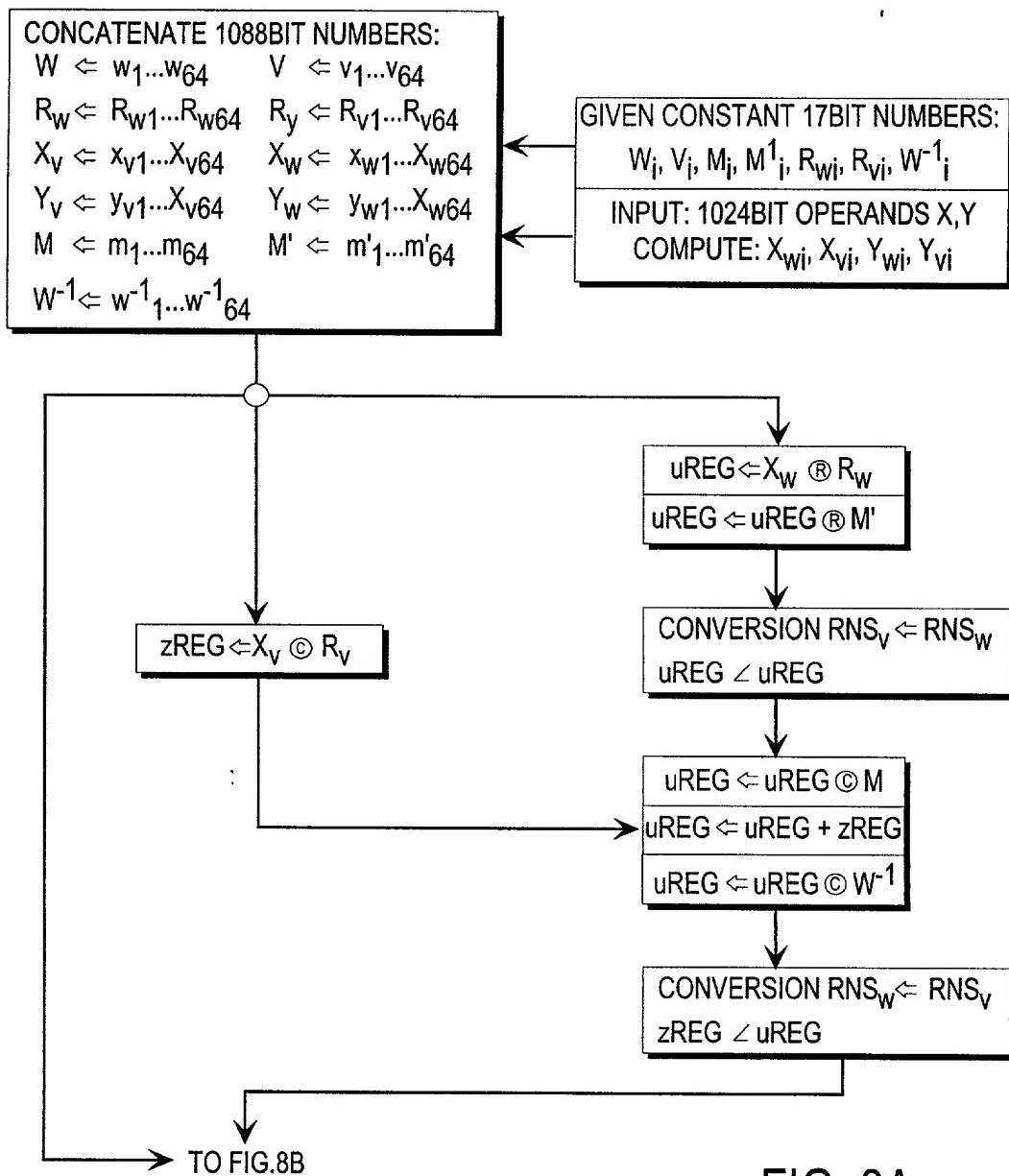


FIG. 8A

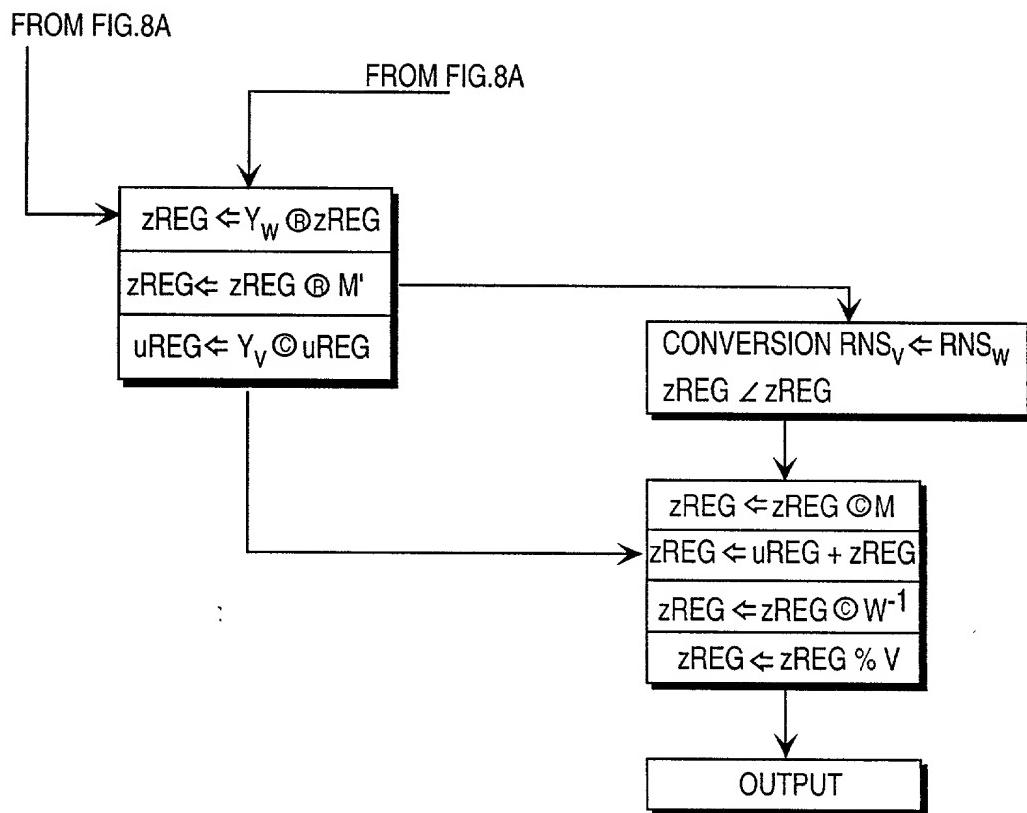


FIG. 8B

NOTE: ALL BUSSES ARE 64 X 17 = 1088 BITS WIDE.

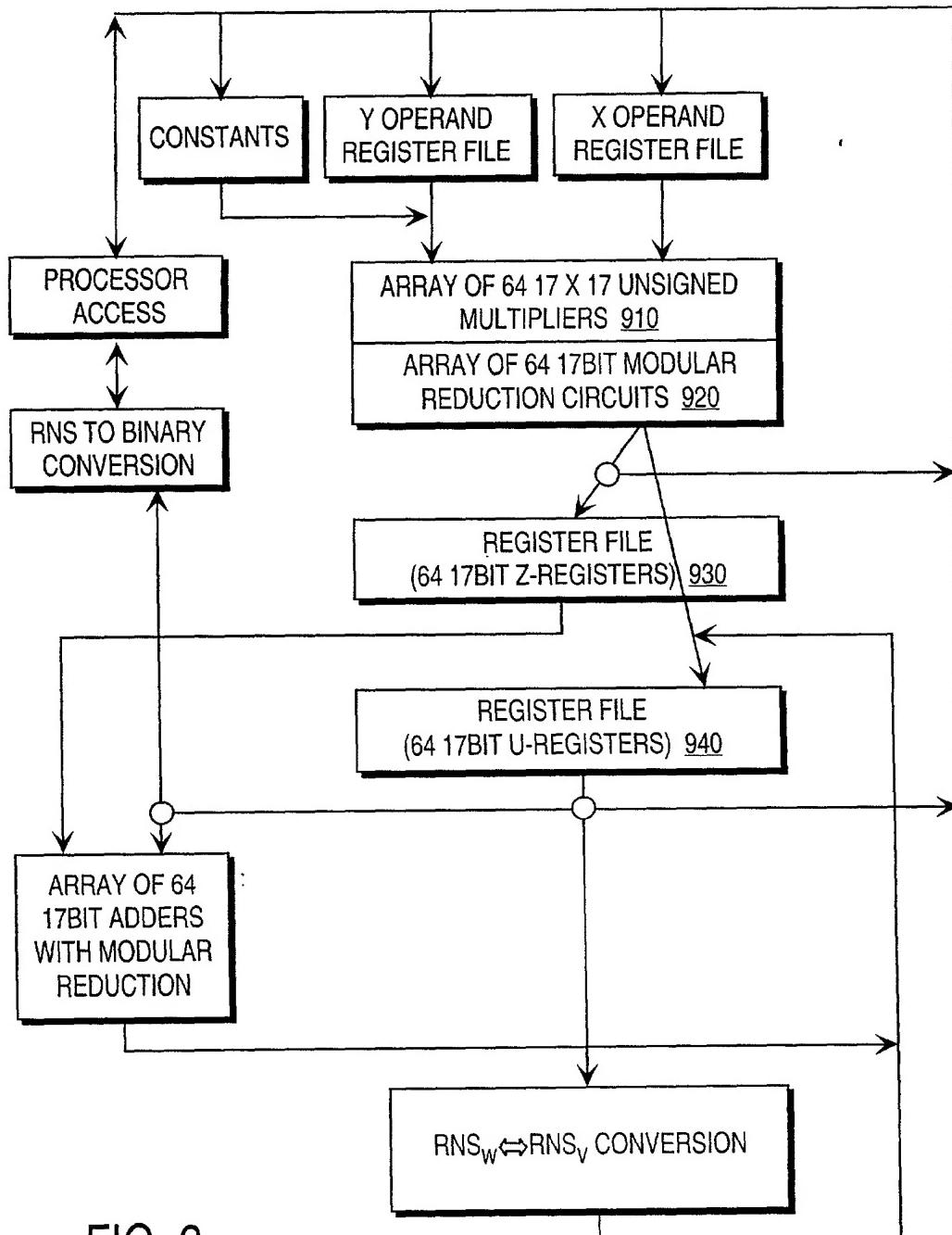


FIG. 9

12 / 28

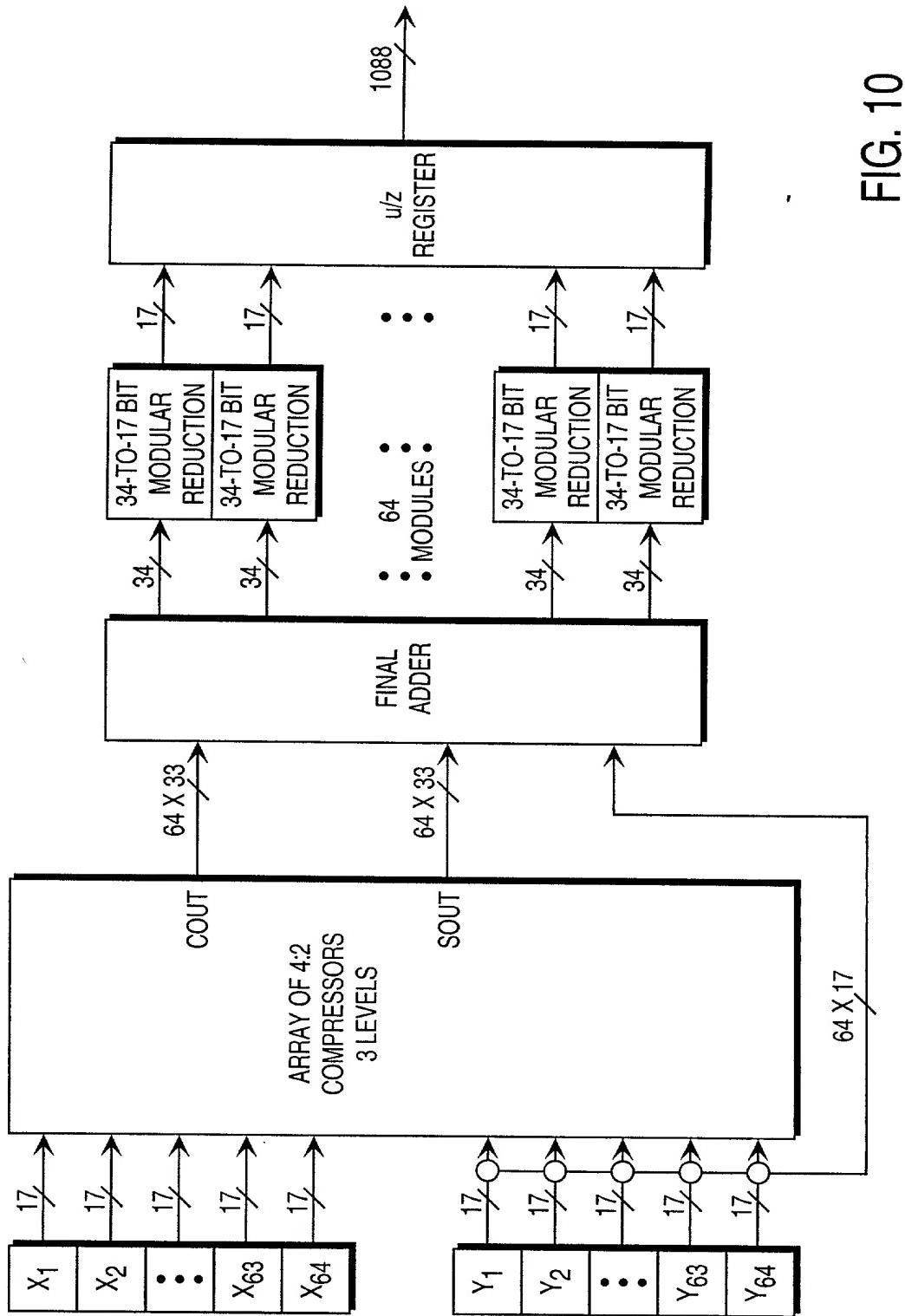


FIG. 10

13 / 28

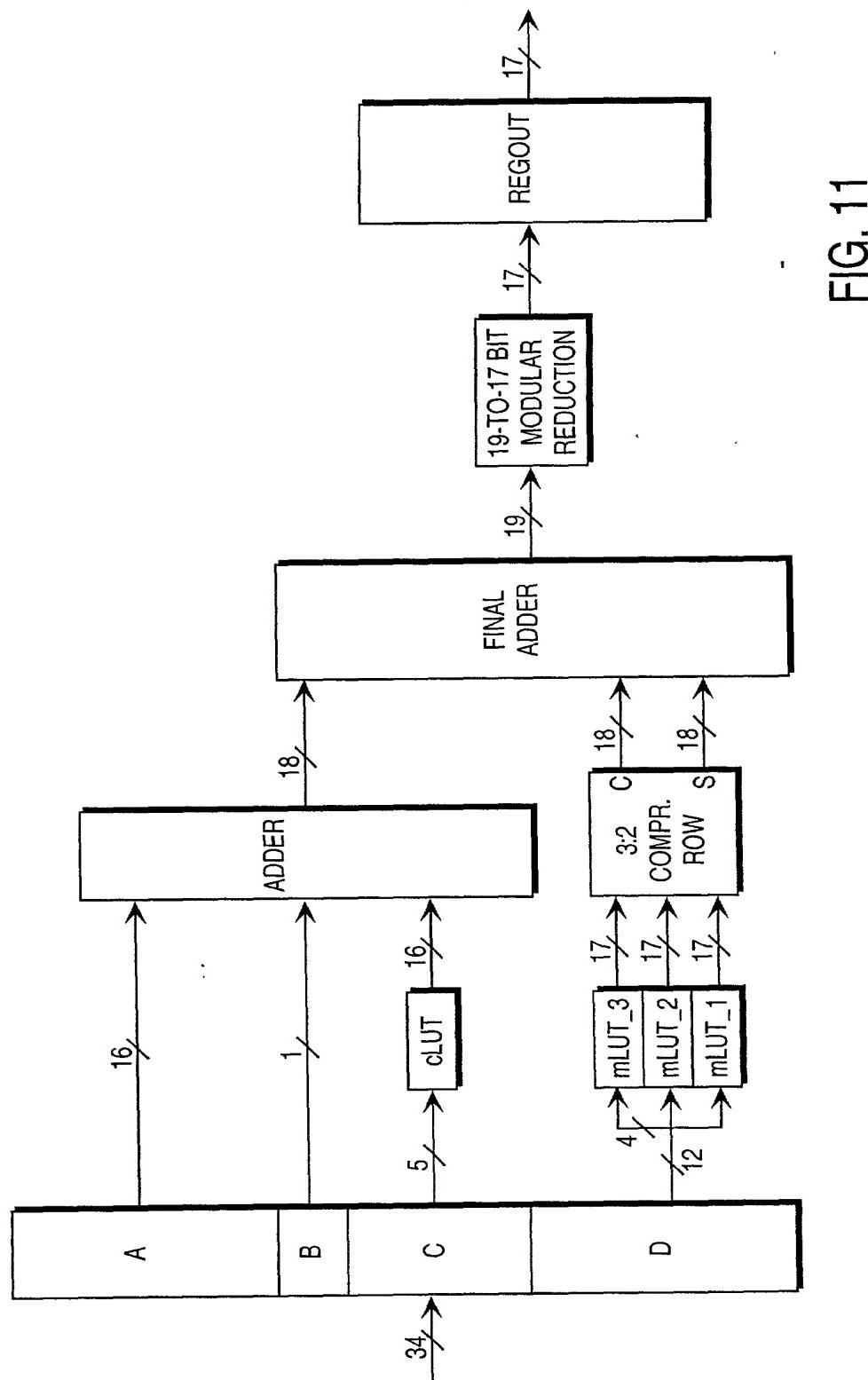


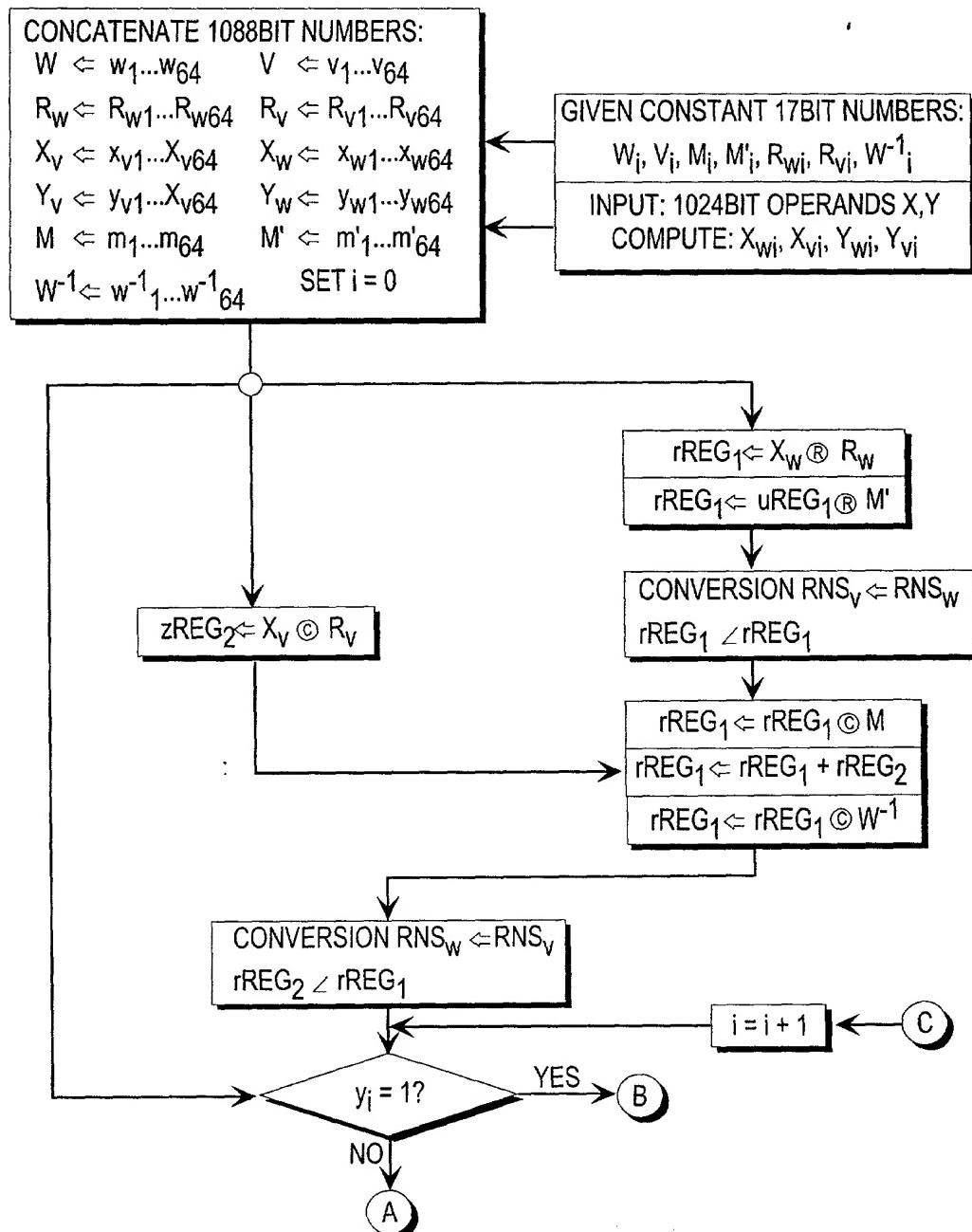
FIG. 11

14 / 28

NOTE: RECTANGULAR BLOCKS ON THE SAME HORIZONTAL LEVEL OVERLAP EXECUTION TIMES.

- ←- SOURCE OVERWRITES DESTINATION REGISTER
- ®- MODULAR MULTIPLICATION WITH RESPECT TO W.
- ©- MODULAR MULTIPLICATION WITH RESPECT TO V.
- ∠- RNS CONVERSION

FIG. 12A



15 / 28

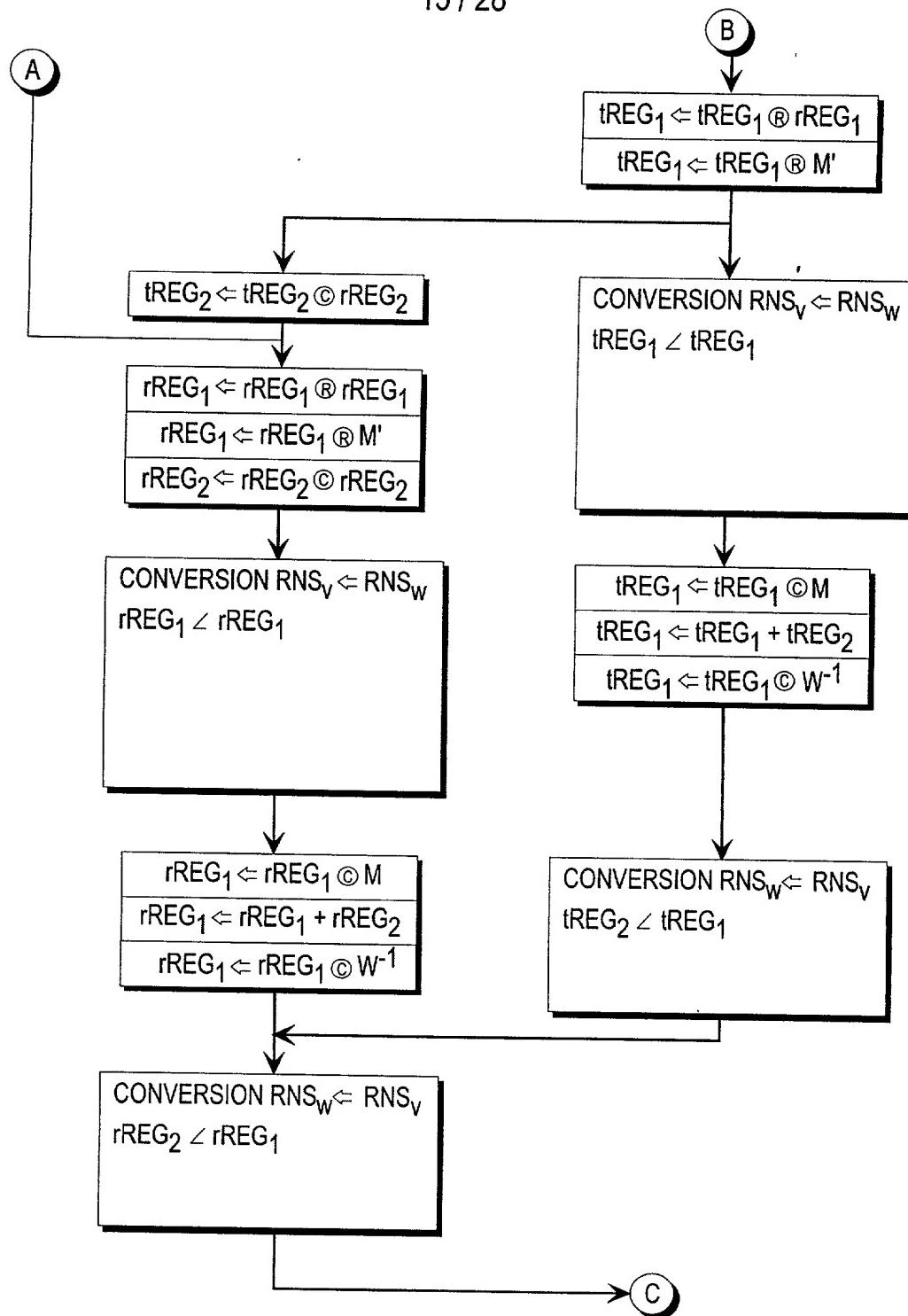


FIG. 12B

16 / 28

NOTE: ALL BUSSES ARE 64 X 17 = 1088 BITS WIDE.

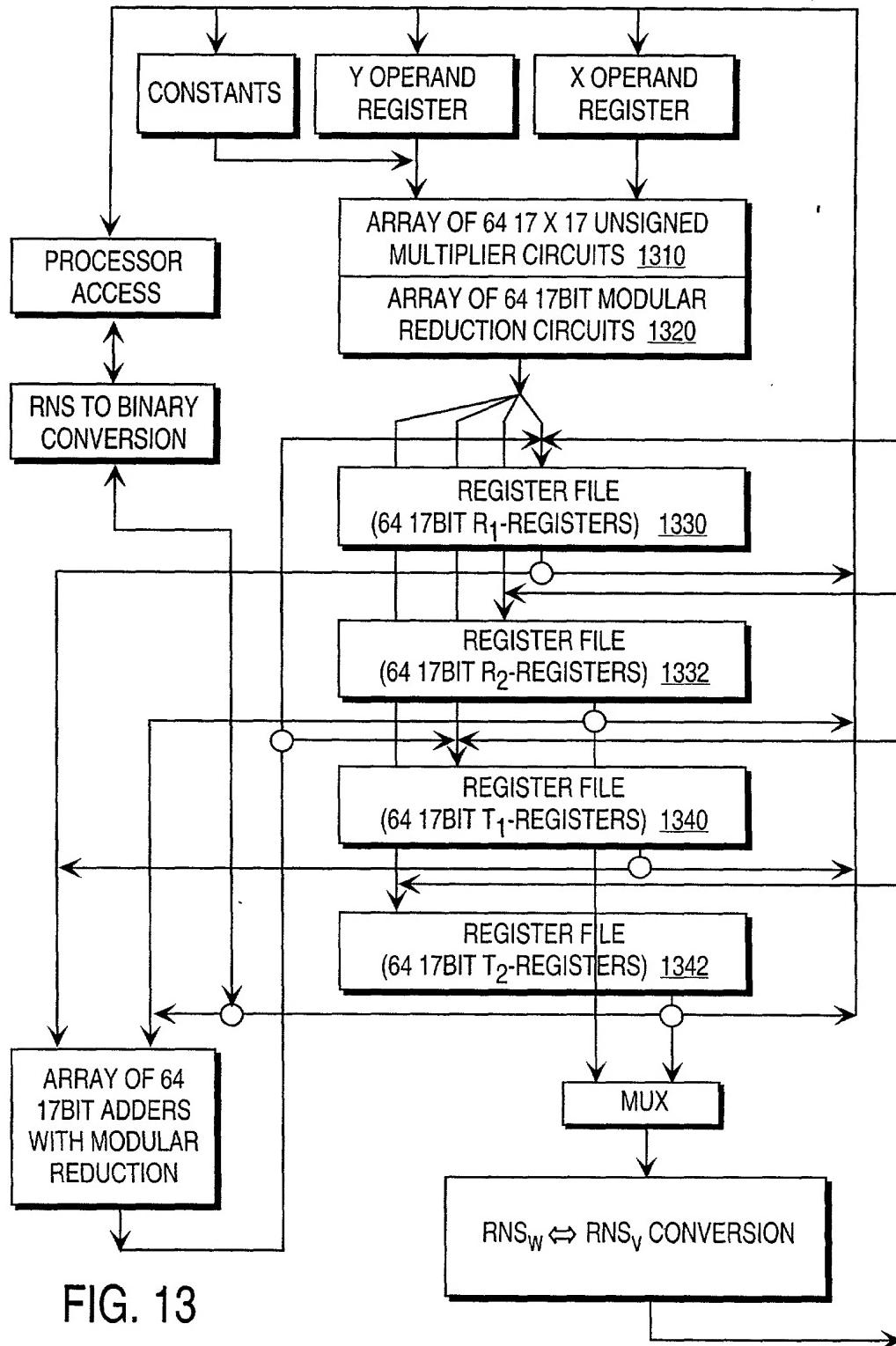


FIG. 13

Title: Pre-Computation and Dual-Pass Modular Arithmetic Operation Approach to Implement Encryption Protocols Efficiently in Electronic Integrated Circuits
Inventor(s): Mihailo M. Stojancic, et al.
Serial No.: 09/955,902
Docket No. 50325-0550

17 / 28

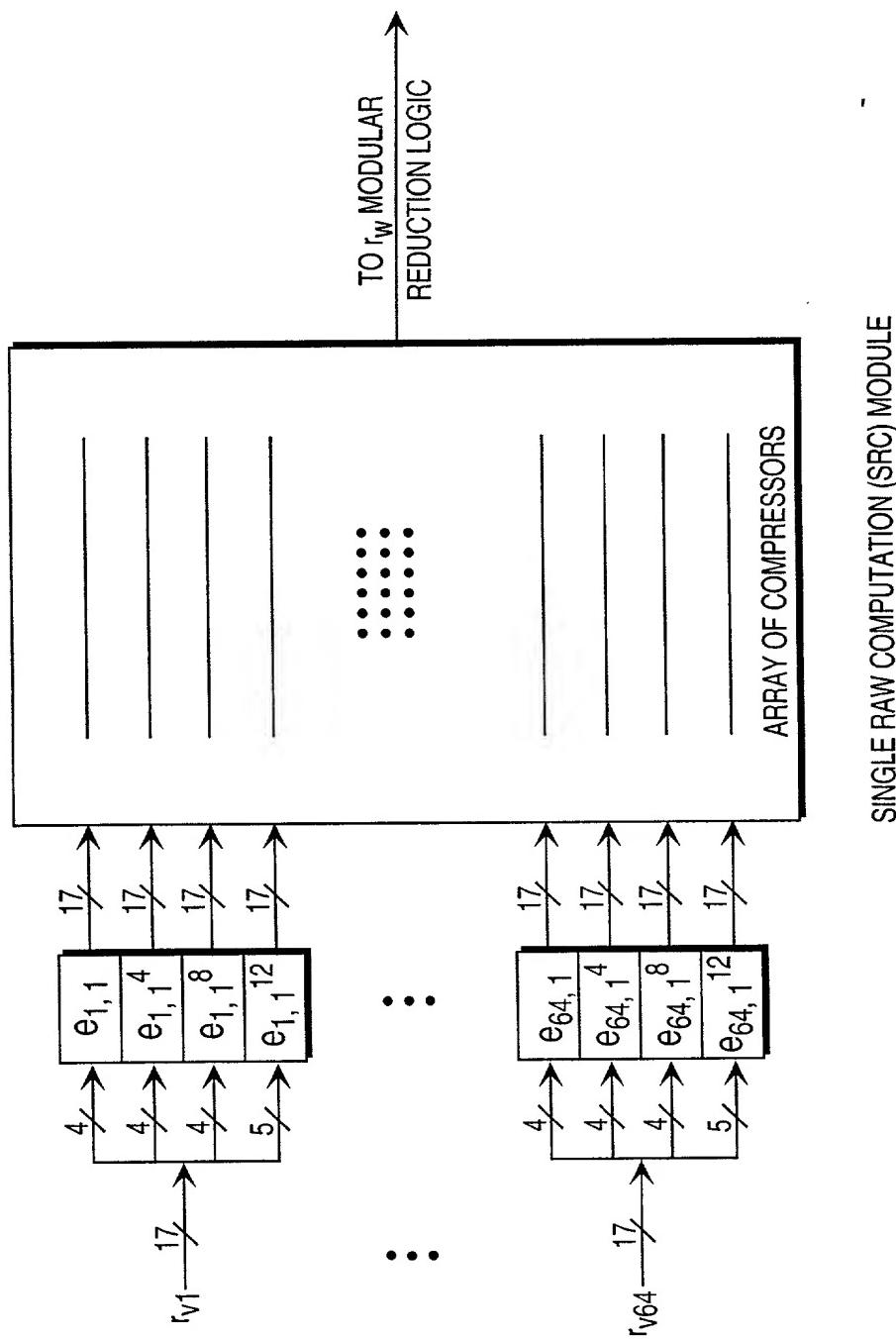


FIG. 14

SINGLE RAW COMPUTATION (SRC) MODULE

Title: Pre-Computation and Dual-Pass Modular Arithmetic Operation Approach to Implement Encryption Protocols Efficiently in Electronic Integrated Circuits
Inventor(s): Mihailo M. Stojancic, et al.
Serial No.: 09/955,902
Docket No. 50325-0550

18 / 28

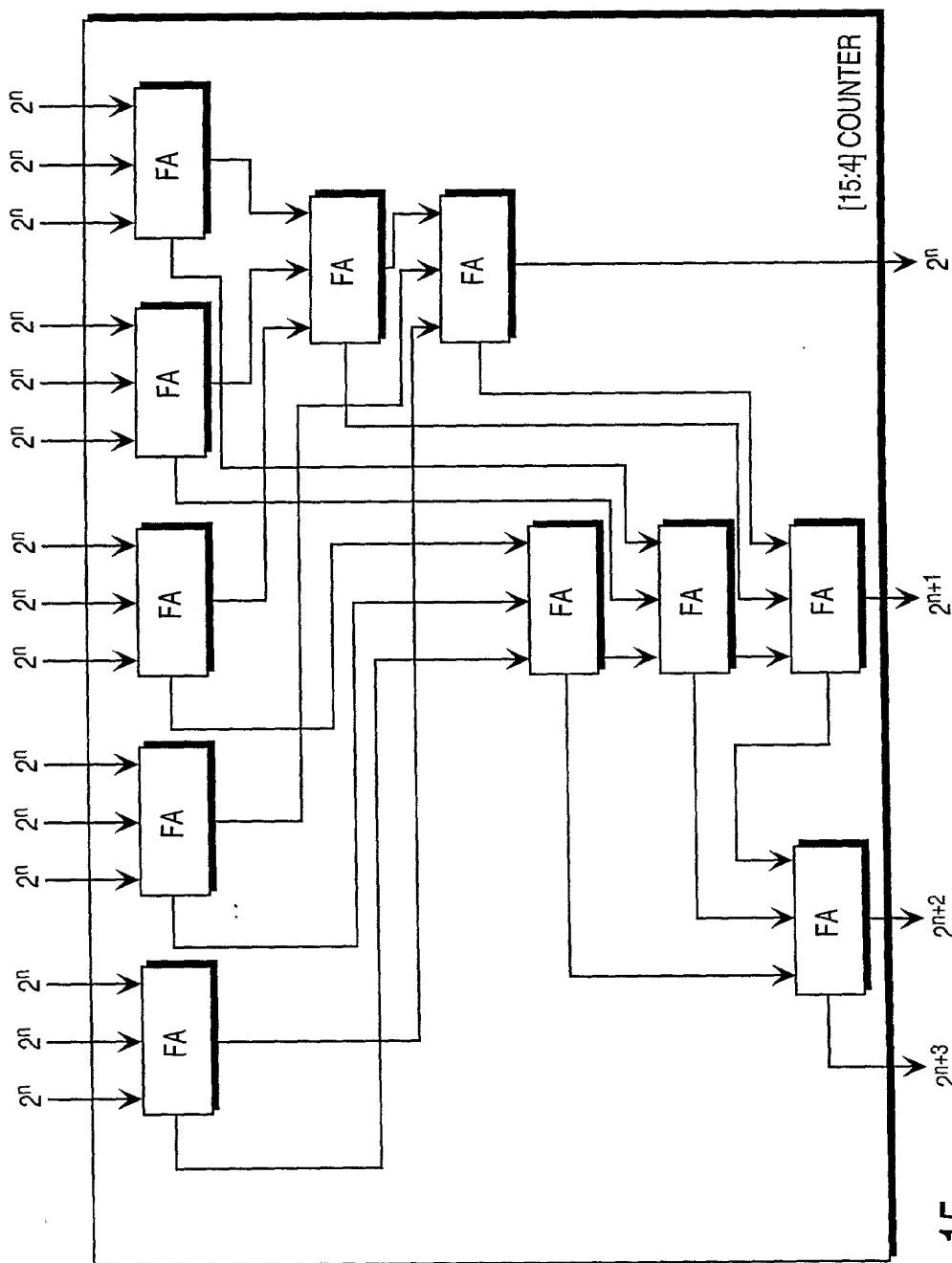


FIG. 15

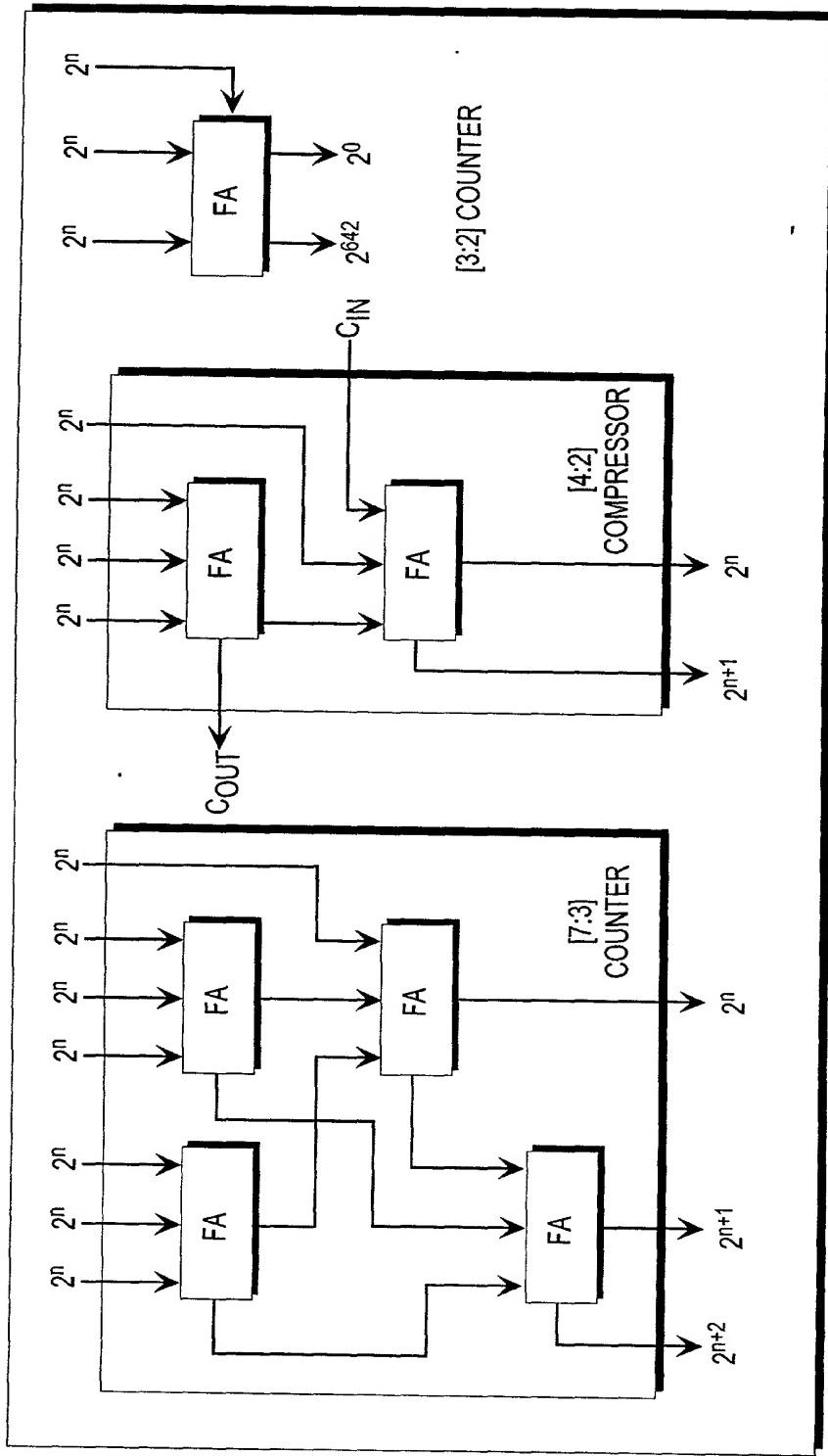


FIG. 16

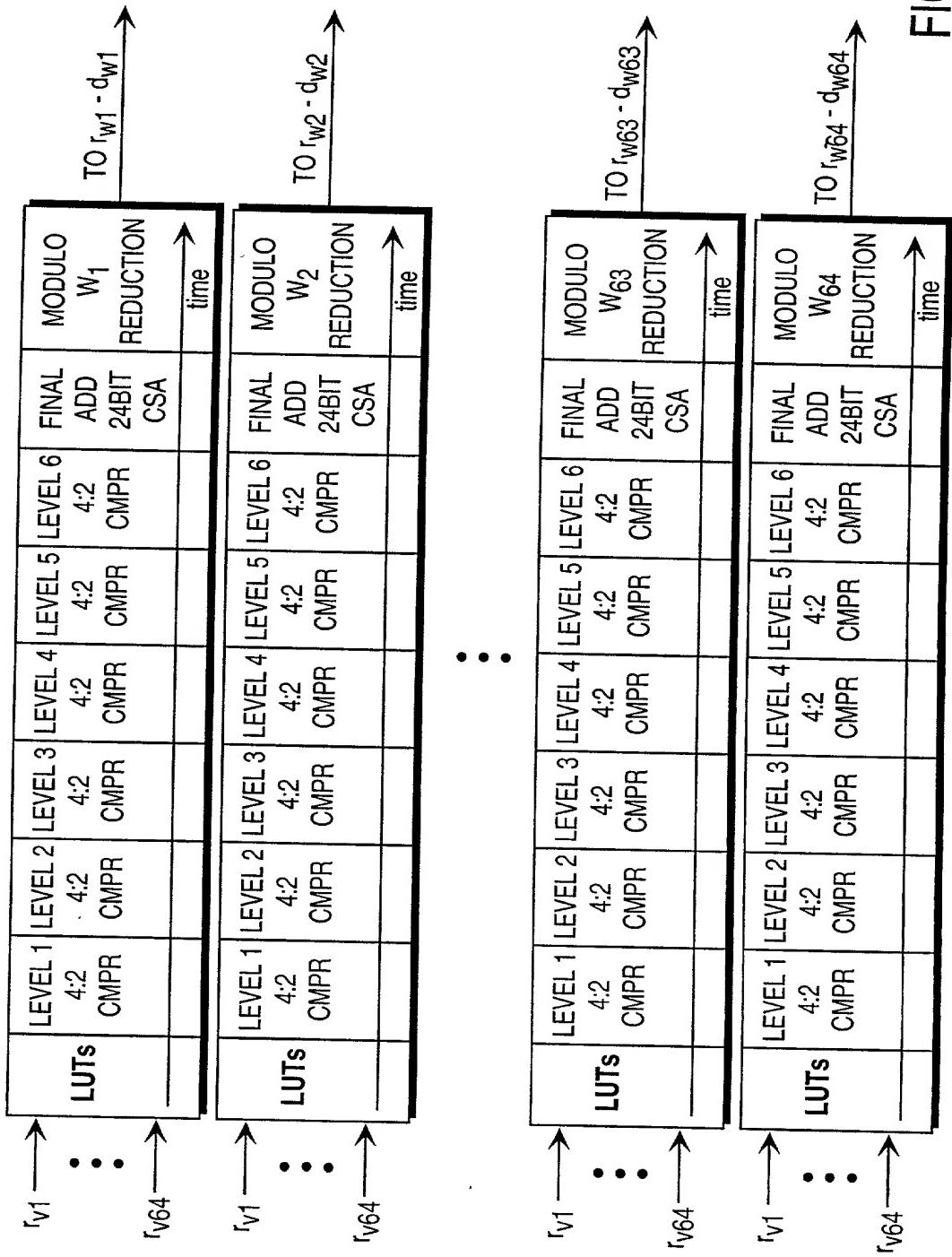


FIG. 17

Title: Pre-Computation and Dual-Pass Modular Arithmetic Operation Approach to Implement Encrypted Protocols Efficiently in Electronic Integrated Circuits
Inventor(s): Mihailo M. Stojancic, et al.
Serial No.: 09/955,902
Docket No. 50325-0550

21 / 28

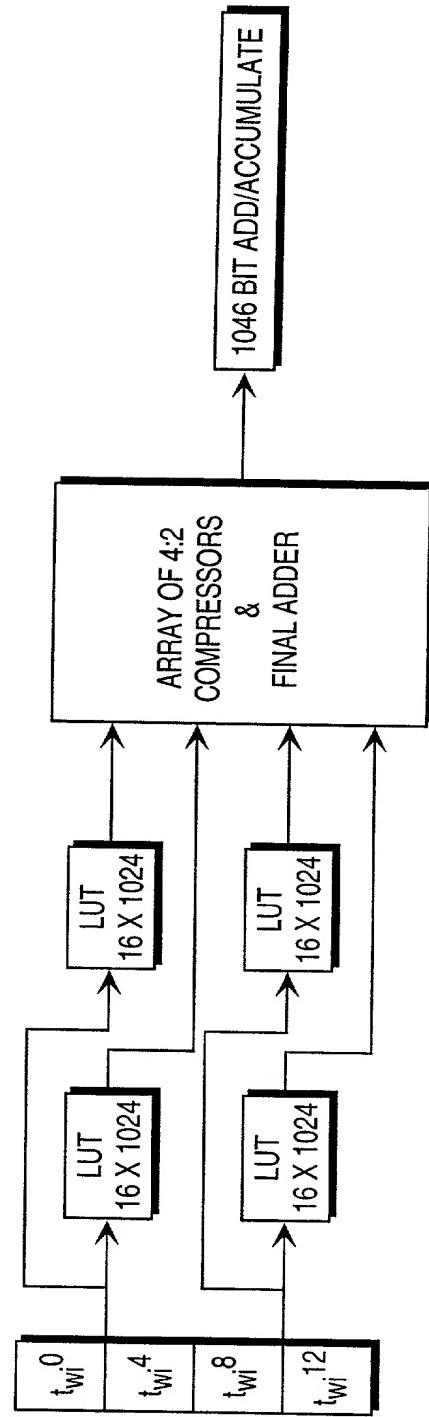


FIG. 18

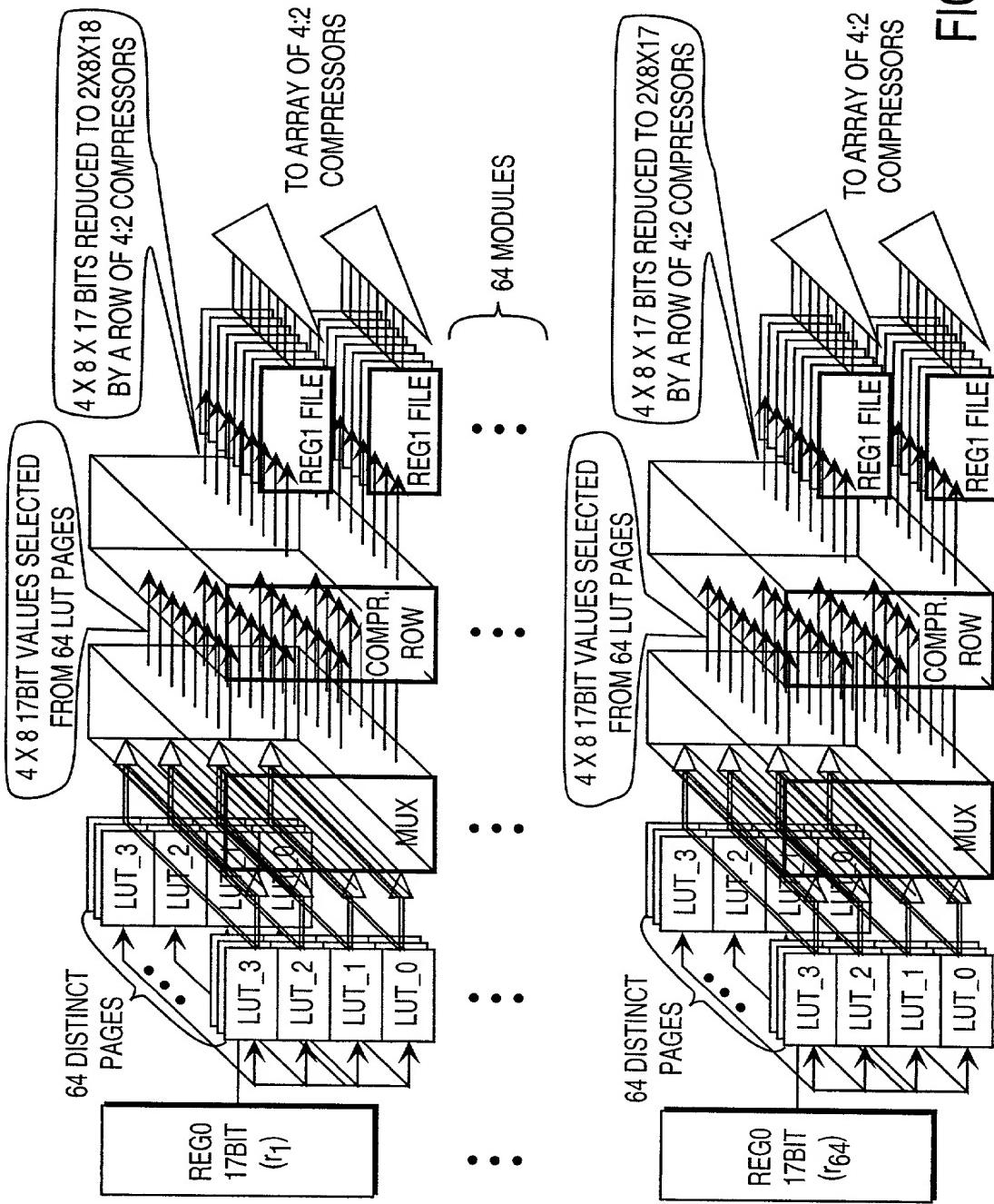


FIG. 19

23 / 28

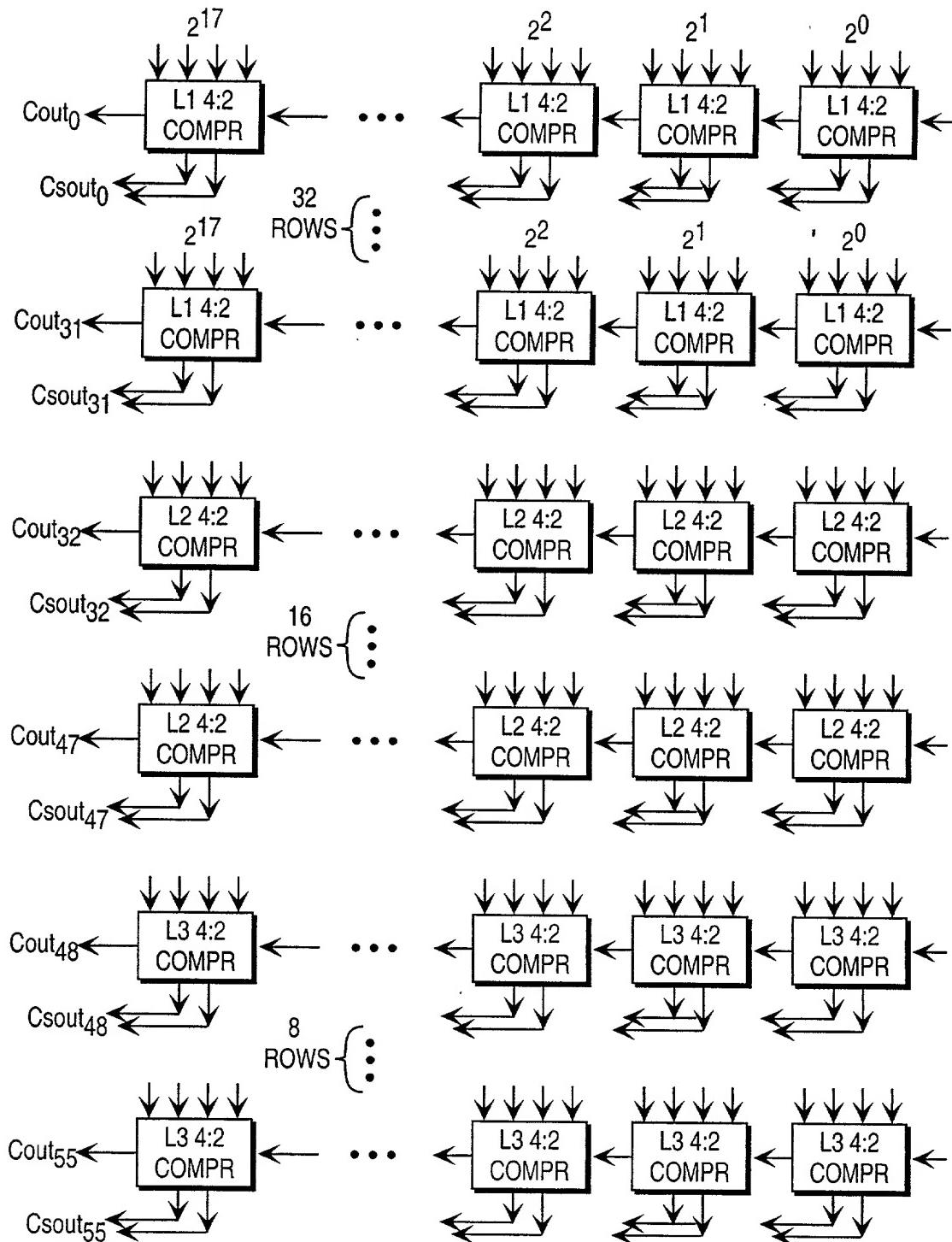


FIG. 20A

CONTINUED ON FIG. 20B

CONTINUED FROM FIG. 20A

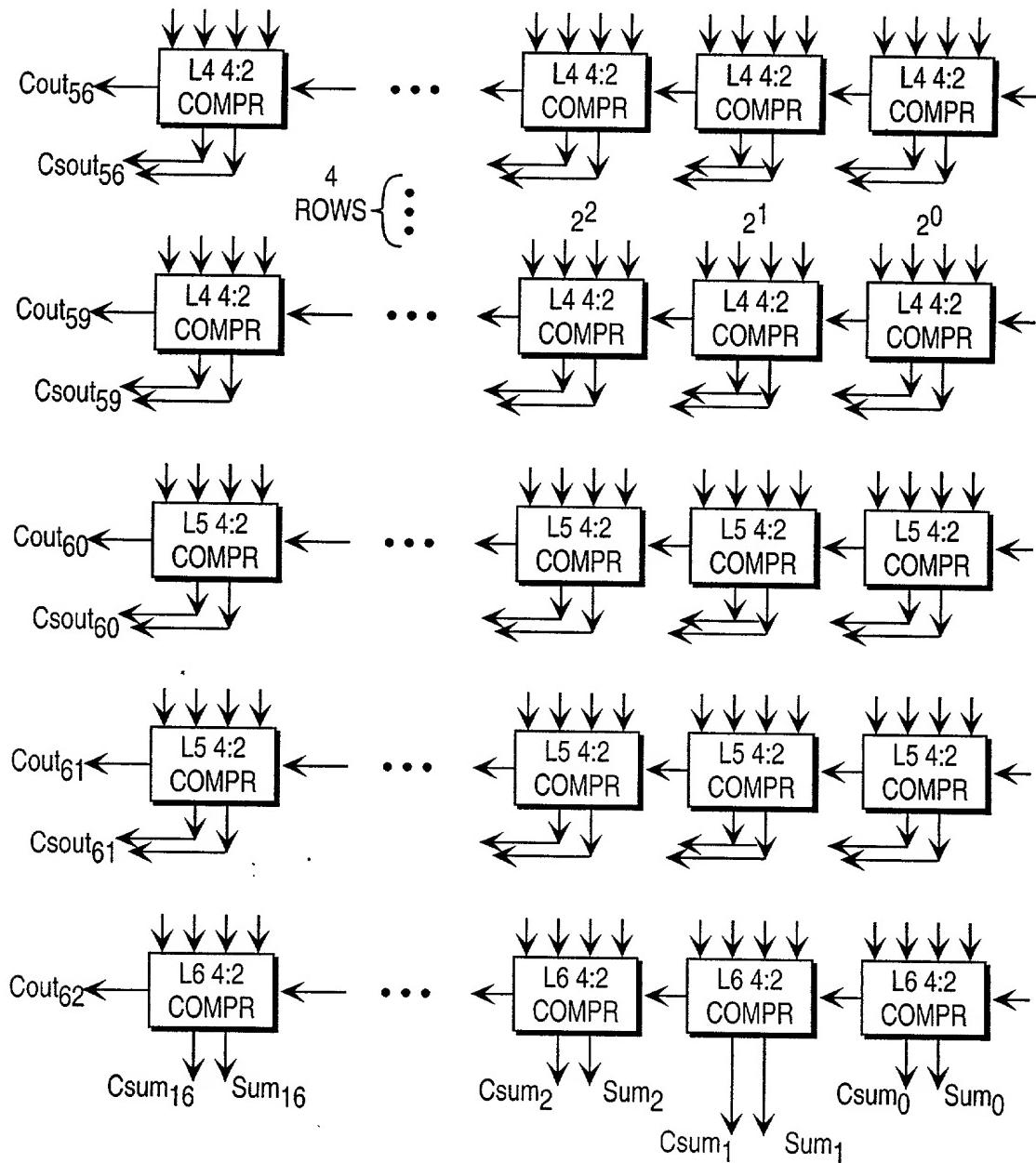


FIG. 20B

Title: Pre-Computation and Dual-Pass Modular Arithmetic Operation
 Approach to Implement Enc./Dec. Protocols Efficiently in Electronic
 Integrated Circuits
 Inventor(s): Mihailo M. Stojancic, et al.
 Serial No.: 09/955,902
 Docket No. 50325-0550

FIG. 21

8 PLANES OF PIPELINED HARDWARE
FOR SIMULTANEOUS EXECUTION

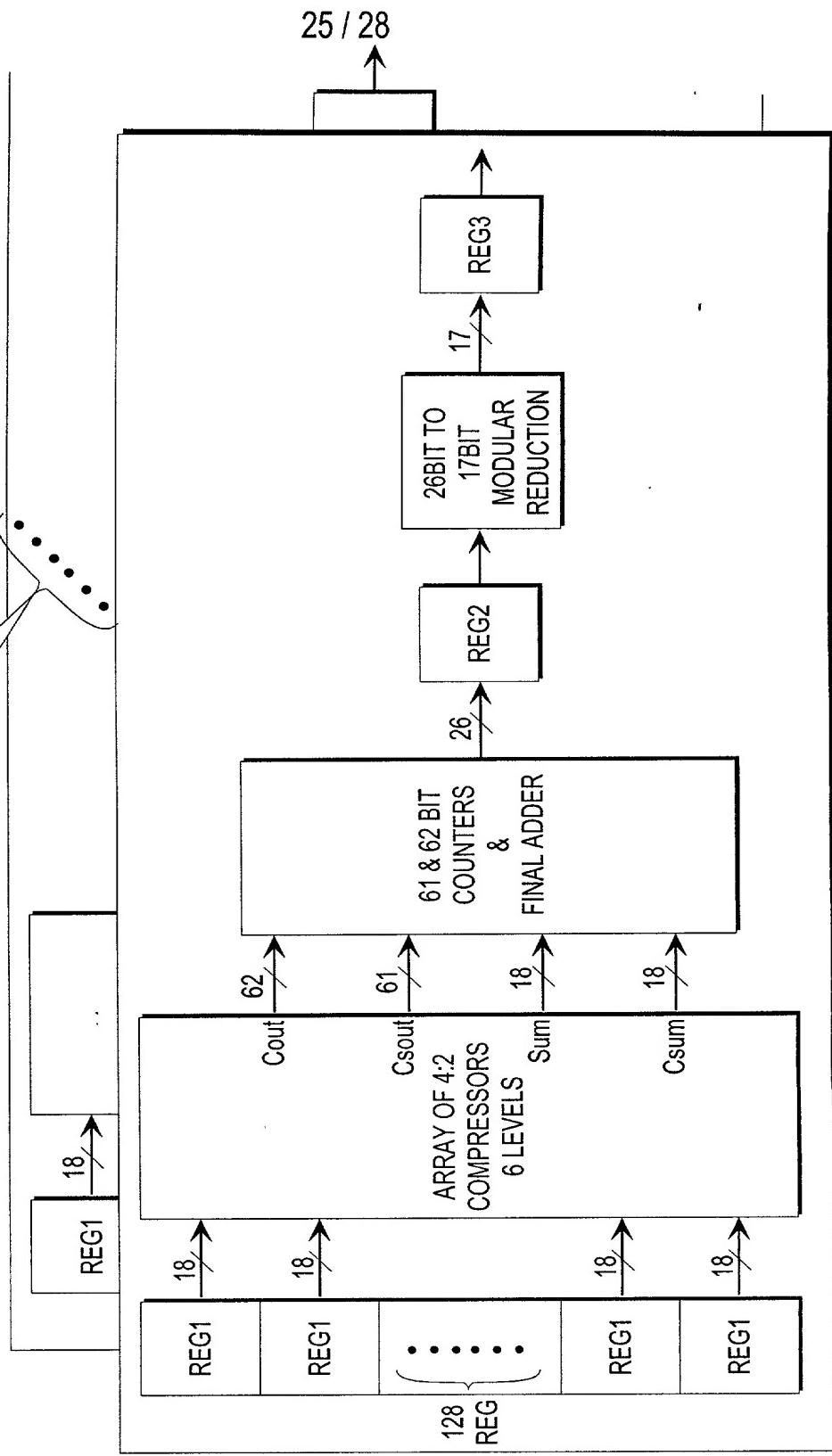
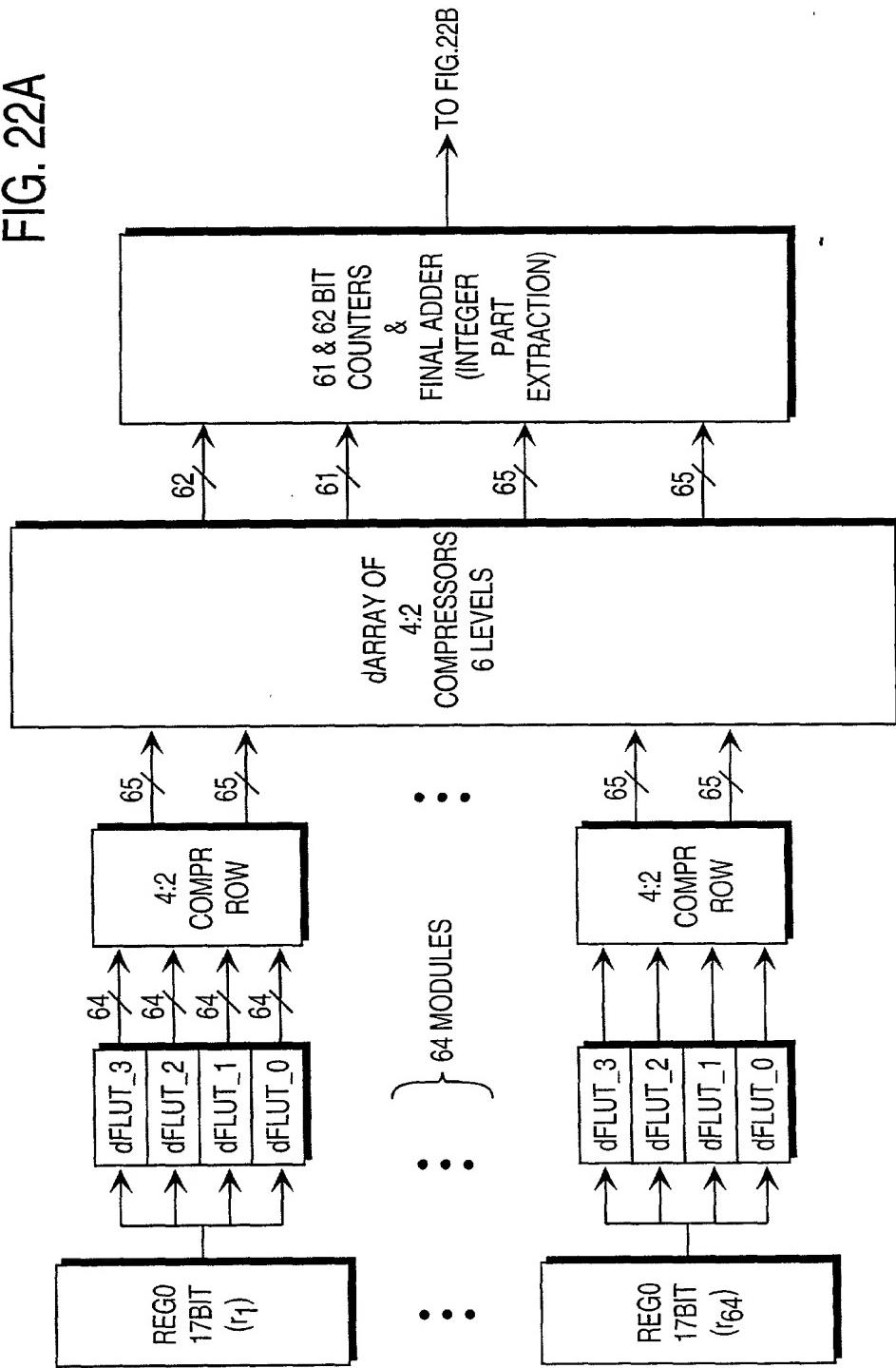


FIG. 22A



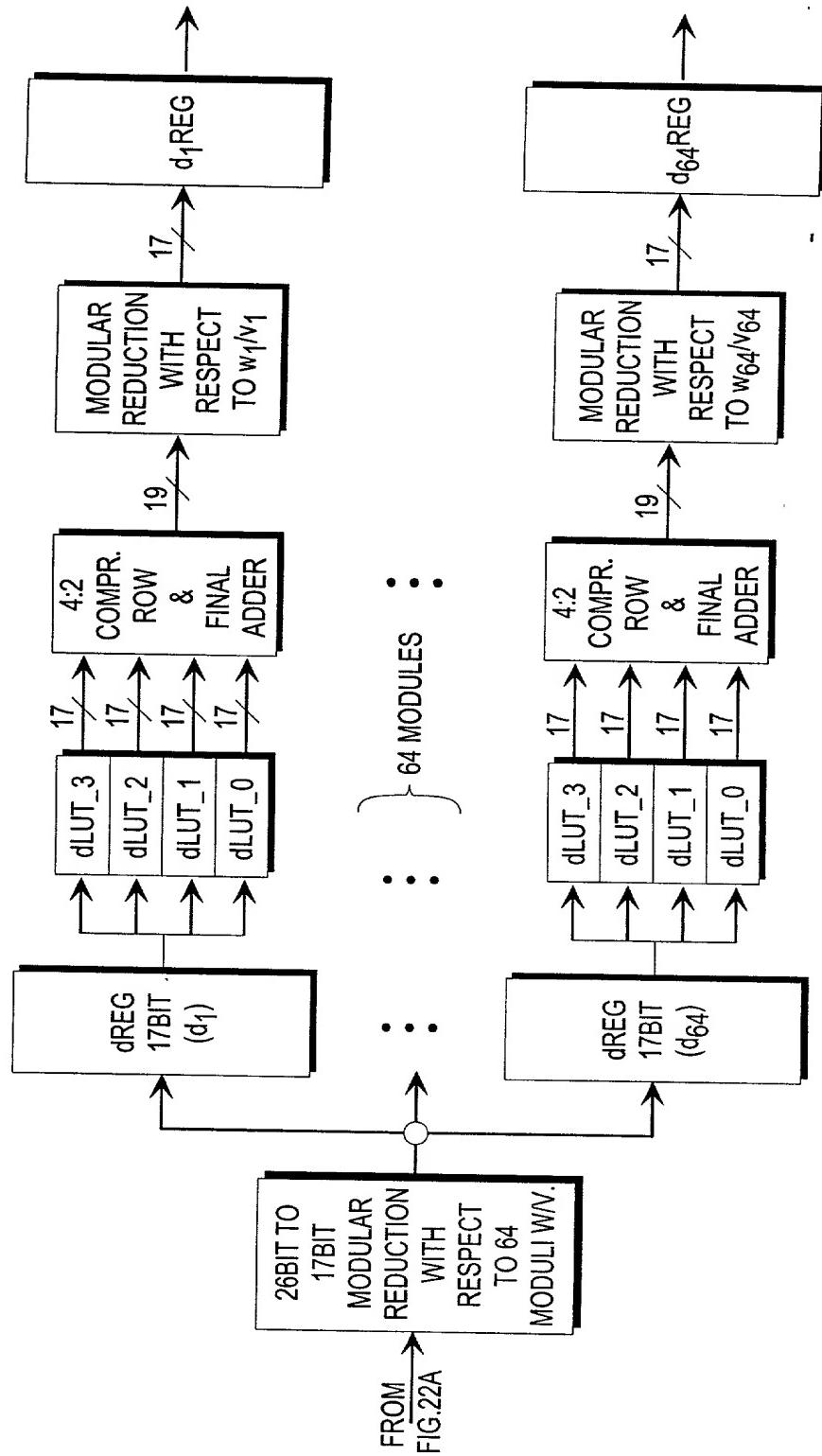


FIG. 22B

28 / 28

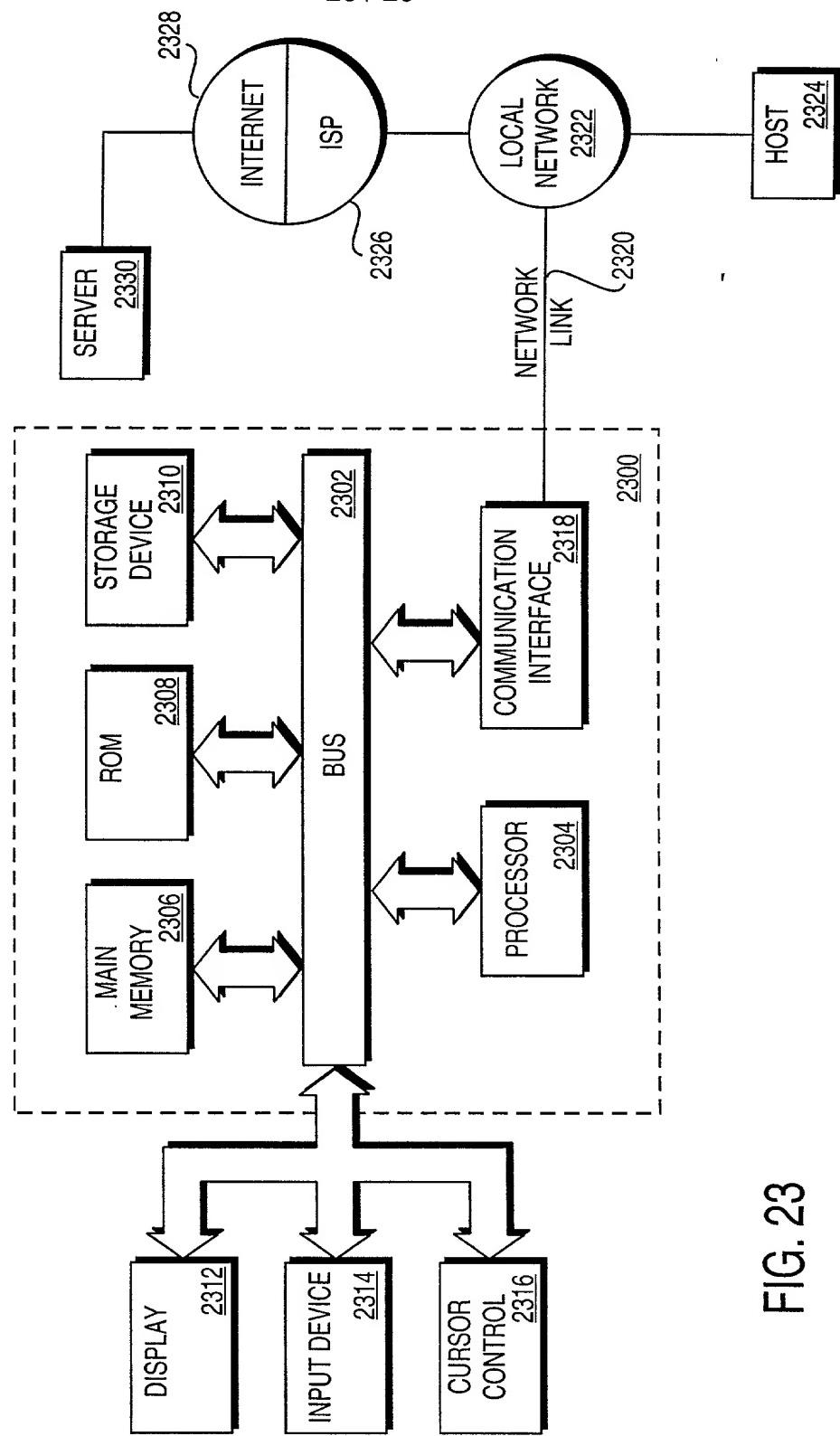


FIG. 23